FLEXERA SOFTWARE

VULNERABILITY UPDATE

November 2015 – January 2016

IN THIS ISSUE

* **Definition of the Top 20:** The Top 20 are the 20 products with the most vulnerabilities in the specified month, out of the more than 50,000 products verified by Secunia Research at Flexera Software, and recorded in the Secunia Vulnerability Database.

The Secunia ID (SAID) identifies the product. Secunia Advisories cover vulnerabilities announced for all types of programs and operating systems.

Total number of new vulnerabilities in the Top 20 over the three month period:*

2,441

Vendor with most vulnerable products in the three month period:

IBM®

Product with the most vulnerabilities:

Avant® Browser

1

Communication and Coordination!

Security professionals and operations teams need to stay on their toes: 2,441 vulnerabilities were reported in the top 20 of most vulnerable products for November, December and January, 2015, respectively. To mitigate the risk these vulnerabilities pose to the infrastructure, IT and Security teams need to stay on top of their environment and know what's in it. One of best ways to stay secure is to make sure that patches are applied when they are available. However, this is easier said than done.

One thing that can seriously complicate security patching is if a vendor releases a patch that does not fix the issue properly. When the vulnerability thus becomes publicly known and the patch is insufficient, it is a potential liability to users of the product. If a vulnerability becomes public knowledge before a patch is ready, enterprises can be vulnerable because hackers could swarm to a vulnerable network like bees to a honeypot to exploit the vulnerability. Organizations that use the vulnerable software would have very limited options to protect their infrastructure.

That's why communication and coordination around the discovery and fixing of vulnerabilities is a critical factor in vulnerability disclosure. With good coordination, which fortunately is what we see in the majority of vulnerability disclosures, the vendor and researcher communicate around the discovery, creation and testing of a patch, which is then released and pushed to the end-users, who can then fix the vulnerability before hackers have a chance to exploit it.

If the coordination is flawed, sometimes a vendor will push out a patch that doesn't really fix the issue, alerting hackers and users of a vulnerability that can be exploited, without at the same time providing the users with the fix required to protect their infrastructures from it.

2

Two Months and Three Patch Cycles to Fix Windows Vulnerabilities

Jump to Microsoft, a vendor so large and so used to dealing with notifications of vulnerabilities in their products, that the Security Industry literally sets the calendar by their regular patch cycle. However, even an experienced vendor may encounter obstacles when trying to patch vulnerabilities quickly, as the following story shows:

On December 3, Parvez Anwar posted information via Twitter about reportedly previously undisclosed vulnerabilities, which included a link to a ZIP archive containing PoCs (Proof of Concepts) utilizing various Microsoft products as entrance points.

All of these vulnerabilities are considered of the class "Insecure Library Loading" vulnerabilities. Typically such vulnerabilities are rated "Highly Critical" by Secunia Research at Flexera Software, as a user may not be aware that opening for example a RTF (Rich-Text-Format) document in Microsoft Windows may result in the loading of an adjacently placed library on a shared network, which then results in the execution of arbitrary code with the privileges of the user.

In the following two months, Microsoft twice released patches to solve the issue, but to no avail: the patches issued did not fix the vulnerabilities. Despite engaging with Microsoft to address the problems, Secunia Research at Flexera Software had to leave the "solution status" in the Secunia Advisory published to describe the vulnerability, as "unpatched."

It wasn't until Patch Tuesday on the 9th February that Secunia Research at Flexera Software could finally change the solution status from unpatched to **patched** as a proper fix had been confirmed for issues initially reported by Parvez Anwar in December.

It remains to be seen, whether we have seen the end of this specific issue in Microsoft Windows yet. For the professional users, the fact that it took three patch cycles to finally issue a fix that appears to work means triple work – three times, they have to figure out how to best mitigate the vulnerability to protect their organizations. And if the same was the case for all of the 2,441 vulnerabilities discovered, IT teams could just go ahead and cancel all weekends and holidays from now on.

3

Zero-day Vulnerabilities in Microsoft Office and Windows

It hasn't been an easy three months for users of Microsoft products – December also saw two zero-day vulnerabilities in **Microsoft Office** and **Microsoft Windows**. A zero-day vulnerability is a vulnerability that has been actively exploited by hackers, before it is publicly known.

While there's little to do to prevent a zero-day vulnerability being used in an attack against an infrastructure, it is possible to reduce some of the overall threat from zero-days by reducing the rest of the attack surface. This is done by ensuring that all known vulnerabilities in the environment are handled. If all the known vulnerabilities are nicely patched or mitigated, it complicates the hacker's ability to access business critical data. As software vulnerabilities are the root cause of many security issues, understanding how to deal with them is a critical component of protecting any organization from security breaches. Organizations must therefore employ a comprehensive Software Vulnerability Management strategy capable of identifying vulnerable software in the infrastructure, helping IT teams prioritize and assess what to do about them, and providing either the patches to fix them or alternative mitigation strategies.

TOP 20

November 2015

ID	VULNS	PRODUCT
55175	39	IBM Flex System Manager Node (FSM)
36174	28	Microsoft Windows Server 2012
33724	28	Microsoft Windows 8
56872	27	IBM PowerKVM
38138	27	Microsoft Windows RT
59215	26	Microsoft Windows 10
12493	25	Microsoft Internet Explorer
12666	21	Mozilla Firefox
14132	21	pfSense
10134	19	IBM Java
33836	19	IBM WebSphere Real Time
34344	18	Cyberfox
24179	18	Google Chrome
1907	17	Adobe AIR
1674	17	Adobe Flash Player
25664	16	Mozilla Thunderbird
59723	12	IBM MQ (formerly IBM Websphere MQ)
11085	12	Microsoft Windows Server 2008
38592	11	Microsoft Windows 7
14022	11	Microsoft Windows Vista

December 2015

ID	VULNS	PRODUCT
1352	213	Avant Browser
24179	129	Google Chrome
36174	110	Microsoft Windows Server 2012
33724	109	Microsoft Windows 8
38138	109	Microsoft Windows RT
59215	109	Microsoft Windows 10
1674	98	Adobe Flash Player
1907	98	Adobe AIR
2372	64	Apple Macintosh OS X
24592	49	IBM Tivoli Monitoring
31077	44	Waterfox Firefox
10130	43	IBM Hardware Management Console (HMC)
57391	37	Apple iOS
55893	33	Blue Coat Malware Analysis Appliance
28609	33	Wireshark
12493	30	Microsoft Internet Explorer
8691	28	IBM BladeCenter Advanced Management Module Firmware
28141	27	Ubuntu Linux
34434	27	IBM Informix Genero
12666	21	Mozilla Firefox

January 2016

ID	VULNS	PRODUCT
15594	77	Oracle E-Business Suite
55842	65	AlienVault Unified Security Management (USM)
26234	65	OSSIM (AlienVault Open Source SIM)
26184	56	Oracle Enterprise Manager
24179	37	Google Chrome
37914	31	IBM SmartCloud Provisioning
57224	26	IBM InfoSphere Guardium Database Activity Monitor
9488	24	HP Intelligent Management Center (IMC)
56128	23	IBM Tealeaf CX
55671	23	IBM Tealeaf
58502	22	Oracle Solaris 11
12789	22	MySQL
34938	21	IBM InfoSphere Guardium
11864	21	IBM Tivoli Directory Server
56324	21	IBM Security Directory Server
36012	19	IBM Tivoli Composite Application Manager for Transactions
46779	17	Adobe Reader
411	17	Adobe Acrobat
23070	16	cPanel
36351	15	F5 BIG-IP Access Policy Manager

*** Definition of the Top 20:** The Top 20 are the 20 products with the most vulnerabilities in the specified month, out of the more than 50,000 products verified by Secunia Research, and recorded in the Secunia Vulnerability Database. The Secunia ID identifies the product. Secunia Advisories cover vulnerabilities announced for all types of programs and operating systems.

Disclaimer: The data in this report is a snapshot. Because Secunia Advisories are updated continuously, as new information becomes available, data in snapshots taken on different dates may vary.